"Deep Learning Based Intrusion Detection Model for IoT Environment"

A Synopsis Submitted to

Shri Vaishnav Vidyapeeth Vishwavidyalaya

By

MS. BHAGYASHRI BHAGAWAN KOTAME

(Enrolment No: 2005PHDCSE06682)

Under the Guidance of

DR. JIGYASU DUBEY

Professor

Shri Vaishnav Institute of Information Technology,

Shri Vaishnav Vidyapeeth Vishwavidyalaya,

Indore

Research Centre

Shri Vaishnav Institute of Information Technology

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA

Ujjain Road, Indore-453111, M.P.

(2023)

"Deep Learning Based Intrusion Detection Model for IoT Environment"

SUBMITTED BY

MS. BHAGYASHRI B. KOTAME
(Enrolment No: 2005PHDCSE06682)

Supervisor

DR. JIGYASU DUBEY
Professor
SVIIT, SVVV, Indore

DR. SANTOSH DHAR
Dean-Faculty of Doctoral Studies and Research

Document Information

Analyzed document	12-9-22_B.B.Kotame_Synopsis.docx (D144044379)
Submitted	9/14/2022 8:54:00 AM
Submitted by	headlibrary
Submitter email	head-library@svvv.edu.in
Similarity	6%
Analysis address	headlibrary.svvv@analysis.urkund.com

Sources included in the report

W	URL: https://link.springer.com/article/10.1007/s11227-020-03410-y Fetched: 11/6/2021 4:24:17 AM	7
W	URL: https://core.ac.uk/download/pdf/188186001.pdf Fetched: 4/10/2021 7:20:16 AM	1
W	URL: https://www.researchgate.net/publication/330746345_Network_Intrusion_Detection_for_IoT_Securit... Fetched: 6/14/2020 5:09:29 PM	1
W	URL: https://arxiv.org/abs/2007.09342 Fetched: 5/23/2022 8:00:10 PM	1
W	URL: https://www.iieta.org/journals/ts/paper/10.18280/ts.370403 Fetched: 7/15/2021 12:07:57 PM	1
W	URL: https://www.internationaljournalssrg.org/IJCSE/paper-details?Id=388 Fetched: 11/13/2021 2:52:32 PM	2
W	URL: https://www.sciencedirect.com/science/article/pii/S138912862031358X Fetched: 6/5/2022 5:36:01 PM	1
W	URL: https://ieeexplore.ieee.org/abstract/document/9469914 Fetched: 7/18/2022 11:46:31 AM	1
W	URL: https://www.hindawi.com/journals/scn/2021/9938586/ Fetched: 9/26/2021 9:40:43 PM	1
W	URL: https://www.researchgate.net/publication/344468522_DRaNN_A_Deep_Random_Neural_Network_Model_fo... Fetched: 2/10/2021 6:44:24 AM	1
W	URL: https://ieeexplore.ieee.org/document/9308293/ Fetched: 9/7/2022 9:10:38 AM	1
W	URL: https://www.researchgate.net/publication/332729311_Towards_Deep-Learning-Driven_Intrusion_Dete... Fetched: 6/14/2020 5:08:54 PM	1

Entire Document

"Deep Learning Based Intrusion Detection Model for IoT Environment"

TABLE OF CONTENTS

Ser No	Topic	Page No
1.	Introduction	1-3
2.	Rationale	4-4
3.	Literature Survey	5-13
4.	Objective	14-14
5.	Research Methodology	15-15
6.	Conclusion	16-16
7.	References	17-20

LIST OF ABBREVIATIONS		
Sr No	**WORD**	**ABBREVIATIONS**
1.	Internet of Things	IoT
2.	Wireless Sensor Networks	WSN
3.	Intrusion Detection System	IDS
4.	Intrusion Prevention Systems	IPS
5.	Host-based Intrusion Detection System	HIDS
6.	Network-based Intrusion Detection System	NIDS
7.	K-Nearest Neighbor	KNN
8.	Self-Organizing Map	SOM
9.	Support Vector Machine	SVM
10.	War Strategy Shuffled Shepherd	WSSS
11.	Convolutional Neural Network	CNN
12.	Malware Classification with Fine Tune CNN	(MCFT-CNN)
13.	Transient Search Optimization algorithm using the operators of Differential Evolution	TSODE
14.	Feed-forward Neural Network	FNN
15.	Distributed Denial of Service	DDoS

1. INTRODUCTION

The quick advances in technology of communication have made it conceivable to broaden the access of networks from individuals to things and due to inception of the Industry 4.0 integration of intelligent Internet of Things (IoT) sensors has become unavoidable to keep the latest enterprise ecosystem running smoothly. IoT devices have become popular over the last couple of years because of their appealing connectivity, communication, and decision-making features Technical improvement has prompted the novel gradient making unmistakable products learned in the Internet of Things (IoT). It fills as an insight to expand the quantity of actual products, used in regular routines into computerized overlap making the unmistakable articles around in an ecosphere of data. The IoT has purchased all demonstrations of help to be delivered to doorsteps giving superior client support whenever, for anyone, from any place [1].

An empowering innovation chips away at the inter-association of the whole genuinely observed objects that are upheld with the internet on the embedded platform. Therefore, the IoT would be functioning with a huge amount of things that are empowered using the internet. The progressions or the requirements of the internet-empowered actual world are detected and handled with IoT and these are furnished with the essential solutions. The method involved with assembling the data by detecting is where the sensors appear as a piece of IoT.

The Wireless Sensor Networks (WSNs) is an assembling of supreme detecting components combined with communicating, computing, actuating, and power accumulating devices for monitoring the persistent actual world alterations. These groups of autonomous sensors empathize wirelessly causing benefits, for example, minimal expense, restricted power utilization, high versatility with flexibility to unreceptive and brutal conditions managing the cost of them to be associated with IoT to turn into a piece of it, to follow the actual alterations experienced in the objects which are internet empowered.

The traditional techniques for foundation between WSNs with IoT are more energy-consuming and inclined to disappointments as far as the lifetime of the network, bundle conveyance proportion, and postponement [2].

An Intrusion Detection System (IDS) is a protection hardware/software framework, which warns bureaucrats while doubtful movement is found in computers or networks. A few frameworks can make an effort to prevent interruptions and obstruct possible dangers; these frameworks are known as Intrusion Prevention Systems (IPS), however, associations ought to

look as an IPS that can hinder real action because of false positives. As far as reach, an IDS can be categorized into host-based, network-based, or hybrid frameworks. Host-based IDS (HIDS) investigates and observes within computers, for example, application logs, operating system audit records, and key framework documents for dubious action. Network-based IDS (NIDS) supervises the network for dubious traffic and sends in an essential point or different focus in the network [3], [4].

An IDS that can distinguish attacks from host and organization sources is utilizing the hybrid method. As far as discovery technique, an IDS can be arranged into misuse signature-based detection and anomaly-based strategies. The signature-based technique starts by programming an anti-virus that can recognize designs called signatures. This kind of discovery has large exactness as well as less false positive rate for currently perceived attacks however when no example is accessible, identifying the new attacks is troublesome.

The anomaly-based strategy attempts to distinguish obscure attacks by utilizing procedures, for example, machine learning is employed to generate a model of typical and unusual or a class of anomalous exercises and look at the new traffic design against the model. However, the issue with this method is additional time and a higher false positive rate expected to identify peculiarities. Given ongoing distributed scholastic works, anomaly-based interruption identification shows additional promising outcomes in recognizing network attacks contrasted with host-based attacks [5].

Machine learning and information mining have been extensively and efficiently utilized in numerous applications where the training information can be acquired to predict future results [6]. However, numerous machine learning methods are capable fine just under speculation that the preparation information and the testing information both are removed from the comparative probability distribution function and highlight space. At the point when this probability distribution function modifies, the greater part of the models is expected to be recreated from the very outset through recently assembled prepared information. In various applications, it is expensive or not feasible to review the beneficial preparation information to change the models. In such occurrences, transfer learning or information moving among the errand areas would be required.

Transfer learning is used to improve a classifier to gain from one space to one more space by moving the valuable boundaries [7]. With the fast improvement of IoT organizations and the rise of the latest danger types, models based on deep transfer learning, which tackled numerous nonlinear issues, can be utilized as a promising answer for building a reliable IDS for the IoT environment. In particular, in the Industry 4.0 transformation, heterogeneous IoT applications

need an elevated degree of reliable structure of security.

Consequently, there is a requirement for a reliable interruption recognition framework to distinguish malevolent movement inside any heterogeneous IoT network. Steadfastness execution examination incorporates accessibility, proficiency, and adaptability highlights. An IDS model is still up in the air by how frequently it is accessible, and its effectiveness is the way it executes with less computational intricacy. Likewise, scalability is the capacity to adjust effectively to the expanded number of information sources from a more extensive scope of IoT sensors.

2. RATIONALE

In the past twenty years, scientists have utilized various machine learning strategies to upgrade the accuracy and performance of IDSs. These procedures incorporate prediction, regression, outlier detection, association, clustering, classification, and pattern tracking. Instances of these includes K-Nearest Neighbor (KNN) [8], Self-Organizing Map (SOM) [9], Support Vector Machine (SVM) [10], Decision Tree [11] [12]and so on. The major shortcoming of nearest neighbor-based methods is that the typical traffic information does not have a close and adequate number of attack traffic details, the neighbors do not include closeand adjacent number of neighbors. KNN strategy cannot appropriately label the traffic.

Additionally, processing the distance of every object could necessitate complex calculations. The grouping procedures probably did not do excellent in little datasets and active renewing of attack summaries could call for a large number of investment. The factual strategies likewise rely upon certain suspicions about the age of the information in a specific conveyance. In addition, various other issues are also faced by the existing techniques used for detecting intrusions including lack of performance, incompetent to deal with concept drifting contexts, unable to use in the real IoT environment, and also large time consumption [13] [1] [14] [15] [6]. Motivated by the above research, the problems related to energy, precision, recall, and F-measure in intrusion detection of IoT will be taken into consideration while going for the new Intrusion detection model in the IoT environment.

3. LITERATURE SURVEY

The review of literature has been carried out with an aim of researching, the field of use of ML and DL in Intrusion Detection Specifically in IoT devices. Various existing approaches for Intrusion detection in IoT are analyzed in this section.

Mehedi, S.T., *et al.* [1] developed a dependable intrusion detection system on the basis of deep transfer learning together with enhanced performance in contrast with various other prevailing techniques. The first step of this system was pre-processing of data, which has two steps, namely cleaning and integration of data. Then, the data was transformed for achieving more effective resultant practices as well as understanding the patterns simply. The present datasets were transformed into a collective dataset by using a Python script, which comprise the validation and training data. At last, the attack instances were classified within several heterogeneous IoT networks. This approach had the ability to classify the normal and abnormal attack situations precisely devoid of any form of malfunction or experience an action of renovation that kept the accessibility. Furthermore, the properties of scalability were increased by this approach by comprising several heterogeneous reliable sources of data in the training dataset with greatest stability, which were attained from a broad range of IoT sensors.

Raj and Basar , *et al.* [2] proposed a methodology that combines clustering with neural and a straightforward fuzzy rule-based system supported by shortest-path finding ensures to have a route entrenchment with decreased power consumption and improved QOS metrics. To demonstrate its flawless operation, performance study was done in relation to the packet delivery ratio, energy consumption, sensor network life time, and latency.

Paxson , *et al.* [3] presented a standalone system BRO for passively observing a network link through which the intruder's traffic travels in order to detect network intruders in real-time. The design of the system placed a strong emphasis on real-time notification, high-speed (FDDI-rate) monitoring, and extensibility. A "policy script interpreter" decodes event handlers written in a specific language used to represent a site's security policy, and a "event engine" that breaks down a stream of kernel-filtered network data into a sequence of higher level events. The four integrated programs, Finger, FTP, Port mapper, and Telnet, are analyzed by the proposed system.

Roesch, M., *et al.* [4] developed a packet sniffer and logger called snort for lightweight intrusion detection for the networks which is deployed in order to monitor small TCP/IP networks to detect suspicious network traffic for attacks. They spoke about an application where this system is useful as a part of integrated network security. It is a small flexible and

highly capable system for large and small networks.

Atefinia and Ahmadi, *et al.* [5] presented a multi-architectural modular deep neural network model to lower the rate of false-positive intrusion detection systems based on anomalies. The proposed model comprises of a feed-forward module, a stack of restricted Boltzmann machine modules, two recurrent modules, and an aggregator module that receives the output weights from these modules and outputs the model's result. The CSE-CIC-IDS2018 dataset was employed in the model's experiments, and the results suggest that the model may be used in an IDS to provide alerts or stop fresh assaults. In comparison to comparable research, the experimental findings demonstrated an improvement in the detection of various forms of network assaults with accuracy as high as 100%.

Weiss, K., *et al* [6] basically done the survey on transfer learning. Presented information on current solutions and also review the applications which are applied to transfer learning. Stated what is transfer learning, homogeneous transfer learning, Asymmetric features based transfer learning, Symmetric feature based transfer learning, Parameter based transfer learning, Relational based transfer learning, hybrid based transfer learning.

Agrawal et al. [7] Recognized the need that for training data as well as testing data there is need to build high-performance classifiers. They presented deep learning which is useful when enough data is not available in target domain but large data set is available in source domain. They explained transfer learning along with its categorization and also provide someexamples and perspective in association of transfer learning. Also discussed Negative transferlearning in detail along with its effects on accomplishment of learning in target domain.

Chen, C.M., *et al* [8] Proposed an efficient filtering scheme to filter the traffic packets instead of processing all the traffic packets which also leads to reduce the systems workload.

According to them LNID lightweight Network intrusion detection is efficient on detection data and also workload reduction.

De la Hoz, *et al* [9] For anomaly detection they presented a classification approach which hybridizes the statistical techniques and SON for feature selection and noise removal they used principle component analysis and fisher discriminant ratio FDR. To differentiate between the normal and anomalous connection they used probabilistic self-organized maps PSOM. By modifying the unit’s activations probabilities detection capabilities of the system can be modified.

Al-Yaseen, *et al*. [10] proposed multilevel hybrid intrusion detection model which uses extreme learning machine and super vector machine so as to improve the efficiency of detectingthe known and unknown attacks. To build high quality training data set they used modified K-

means algorithm. This modified K-means algorithm.

Kevric, J., *et al* [11] Developed combining classifier model for a network intrusion detection based on tree based algorithms. To evaluate the performance, they used NSL-KDD dataset. They used 41 features to classify weather incoming traffic is attack or normal. They used combination of random tree and NBTrees algorithm and detection accuracy achieved was 89.24%.

Sahu, S., *et al* [12] Used Kyoto 2006+ dataset which at every instance is labeled as normal attack and unknown attack. They used J48(Decision Tree) to classify the packets in network which can be used to NIDS for training and testing they used 134665 network instances. The rules they generated gave accuracy of 97.2%.

Fatani, A., *et al.* [13] developed an effective technique for IDS by utilizing the benefits of metaheuristics optimization and deep learning algorithms. For the process of extracting appropriate features from the datasets, a feature extraction method was developed on the basis of CNN. Then, a novel variation of transient search optimization algorithm was developed and it was named as TSODE. It was developed by utilizing the operators of differential progression, which were utilized for enhancing the exploration stages in addition to multiplicity of the agents of the conventional transient search optimization and to avoid its limitations.

Idrissi, I.,*et al.* [14] developed a technique for intrusion detection by using deep transfer learning. This approach had six phases of process, and it used two datasets, so the initial two phases were pre-processing of these two datasets. In the third phase, the developed model was build and trained on a training dataset. After that, the model was evaluated on the new dataset for predicting attacks in the fourth phase. In the fifth phase, the convolutional base was freeze up by the original as well as already trained model and its output was used for feeding the classifier. In the final phase, the updated model was evaluated by the prediction of attacks.

Tien, C.W.,*et al.* [15] established a machine learning method for intrusion identification in smart factories. Initially, the framework was designed in order to collect the packets of network created from tools and investigate the arriving packets for detecting intrusion at the boundary of the network. It was assumed that, the anomalies of device were decided from the generated packets. After identification process, the normal and abnormal behaviors were distinguished. The unsupervised learning method was adopted for learning the significant features for the chosen types of device. The adopted method comprises isolation forest, auto encoder and one-class SVM to reduce dimensionality. At last, the auto encoders were utilized for transfer learning to deploy the learned model from one site to another site for anomaly detection.

Deng, L., *et al* [16] introduced a novel scheme for intrusion detection in IoT, which was light

weight intrusion detection technique merged with Principle Component Analysis (PCA) and Fuzzy C Means (FCM) algorithm. PCA was referred as an algorithm for dimension reduction. It was used in the face of large quantity of information and complex systems, for eliminating the unnecessary data included in it and for retaining the required data. Feature selection of intrusion detection utilized by PCA algorithm, for decreasing the amount of features of the system process, and limiting the time of detection. The dataset was divided into C fuzzy clustering sets by the FCM, it made the objective function of the non-similarity index was low. Sudhakar and Kumar, S., *et.al.* [17] presented an MCFT-CNN model for the prediction of strange malicious software variants exclusive of feature engineering and former understanding of reverse engineering or analysis of binary code. A comprehensive investigation of the model was performed by the tuning of several hyper parameters. Then, the model was trained with the transfer learning by means of the dataset. Next, for comparing the categorization report of this method with ResNet50, an experimental method has been utilized.

Ge, M., *et al* [18] developed an innovative approach to detect intrusions against cyber-attacks for the networks of IoT on the basis of the conception of deep learning. The classifier was designed as a FNN model with layers of embedding for identifying four classes of attacks, known as information theft, reconnaissance, Distributed Denial of Service (DDoS), and Denial of Service (DoS) when distinguishing these from the genuine network traffic. Additionally, the encoding of high dimensional definite features was extorted during embedding of network as well as applied for binary classifier through transfer learning. Four classes were considered for the multiclass classification since it was observed that the developed model acquiesce sub-par performance for definite sub-classifications of attacks.

Ullah, I. and Mahmoud, Q.H., [19] designed an anomaly based intrusion detection model for the network of IoT by the use of CNN architecture in the multiclass classifier for effective categorization of attacks and differentiating them from normal network traffic. A new dataset was generated in this approach from an existing dataset. Four IoT datasets were generated by using the developed method, and then they were grouped for increasing the amount of attack classes. A range of anomalies were classified by means of one dimensional, two dimensional and three dimensional CNN models. Moreover, the principle of transfer learning was utilized to construct multiclass as well as binary categorization models. The developed multiclass as well as binary categorization model attained recall, precision and accuracy.

Sharmisth et al. [20] have proposed model for detecting attacks in Lossy Networks and the Routing Protocol (RPL). To compare the performance improvement of the Generative Adversarial Network-Classifier (GAN-C) with a standalone Support Vector Machine (SVM)

classifier, a method called Generative Adversarial Network-Classifier (GAN-C) was proposed for attack detection events. The suggested approach uses a parallel learning and detection model that facilitates DL on IIoT devices with limited processing capacity. In order to comparethe performance of distributed and centralized attack detection in an RPL network, the outcomes of the parallel model were assessed in an IIoT network.

T. Ayyarao et al. [21] proposed War Strategy Optimization (WSO) method based on traditional military tactics based on strategic movement of army soldiers during a conflict during which the direction of the combat plan was modelled for optimization. Attack and defense battle tactics were modelled by the developed algorithm, according to the which the soldier placements on the battlefield were proposed. A weight updating technique and a weak soldier's relocation strategy to improve the algorithm's efficiency and endurance. The suggested algorithm's effectiveness was examined using 50 benchmark functions and four engineering challenges. Ten metaheuristic algorithms are being used to evaluate the algorithm'sperformance. The outcomes of experiments on various function optimization proved the superiority of the suggested approach.

A.Kaveh ,A. Zaerreza[22] presented a new multi-community meta-heuristic optimization algorithm, called shuffled shepherd optimization algorithm (SSOA). The agents are firstly separated into multi-communities and then optimization process is performed in order to mimic the behavior of a shepherd in nature operating on each community. Then a new multi-community meta-heuristic optimization algorithm is developed called as shuffled shepherd optimization algorithm and also applied to few attractive examples.

Jain and Bhandare, *et al.* [23] suggested perturbation technique to protect accuracy and privacy as Data mining systems hold a significant quantity of sensitive and private information and needs to prevent data leaking. For the method individual data value were distorted before data mining application for min and max normalization transformation based data perturbation. The findings of the proposed method demonstrated that the performance of the data mining methodology after data distortion is improved by the utility measure and the privacy parameters used for measuring privacy protection.

Shi et al. *et al.* [24] presented a deep Convolutional Neural Network (CNN) based transfer learning algorithm to reduce FP in the detection of pulmonary nodules on CT slices. The method employed a support vector machine (SVM) for nodule classification and one of the most recent CNN models, VGG-16, as a feature extractor to collect nodule features. The CNN model then was tweaked to adapt to the categorization of pulmonary nodules job using the final fully linked layers. Using the training data, such as the pulmonary nodule patch images and

associated labels, the original CNN filter weights were then improved by back-propagation such that they more accurately represented the modalities in the pulmonary nodule image dataset. Results revealed that the suggested method's overall sensitivity was 87.2% with 0.39 FPs per scan, above the 85.4% with 4 FPs per scan attained by competing approaches.

He, K., Zhang, X, *et al.* [25] To make easy the training of networks that are substantially deeper than those used previously they present a residual learning framework. Instead of learning unreferenced functions, they explicitly reformulate the layers as learning residual functions with reference to the layer inputs. To show how these residual networks are easier tooptimize, and can gain accuracy from considerably increased depth they provide comprehensive empirical evidence.

BoT-IoT dataset [26] it states about the BoT-IoT data set that was created by designing a realistic network environment in the Cyber Range Lab of UNSW Canberra. The network environment included a combination of normal and botnet traffic. Source files of the dataset are provided with different formats, including the original pcap files, the generated argus files and csv files. The also included DDoS, DoS, OS, Service Scan, Keylogging and Data exfiltration attacks, with the DDoS and DoS attacks further organized, based on the protocol used.

Y. Zhang, *et al.* [27] Designed the model for Intrusion Detection based on improved genetic algorithm and deep belief network. Initially by facing various types of attacks by multiple interactions through genetic algorithm most optional hidden layers and count of neuron at every layer is generated that's the reason why its model based on deep belief network gets very high, detection rate. For simulation and evaluation purpose NSL and KDD data set is used. This model can be used not only for Intrusion detection but also for classification and recognition purpose.

A. Nagisetty, *et al.* [28] Worked on framework in order to detect malicious activities in IoT by using the concept of Keras Deep Learning library. They used multilayer perceptron (NLP), Deep Neural Network method i.e ANN Autoencoder and Convolution Neural Network(CNN) to detect attacks. They used UNSW-NB15 and NSL-KDD99 for performance evaluation and the results are checked based on accuracy, RMSE and F1 score.

M. Zeeshan, *et al.* [29] worked on the concept of Data drift and concept Drift for Intrusion detection in IoT. Data drift states Changes that takes place in relationship among the independent features whereas the Concept drift states the changes that takes place in relationship among input and output data. Developed drift detection technique which capitalizes on method of principle components analysis (PCA) to check the changes in features in Intrusion detection data streams. Also states that their solution stables performance of

intrusion detection on training as well as testing data.

S.Shinly, *et al.* [30] used KNN K-Nearest Neighbor and long short term memory (LSTM) in model for attack detection and performance is checked based on comparison of detection time, kappa statistic, geometric mean and sensitivity. Dataset they used to check effectiveness is BOT-IoT dataset

N. Chaabouni, *et al.* [31] Survey of Intrusion detection in IoT was done. By evaluating the existing defense technique, they classified the IoT security threats and challenges. They did survey on analyzed and compared state-of-the-art Network intrusion detection proposals in the IoT context associated with the Architecture, methodologies, validation strategies, treated threats and algorithm development. They dealt with both traditional and machine learning NIDS techniques.

Mrs.G.Parimala, *et al.* [32] Proposed new feature selection algorithm for identifying most useful features from database that is conditional random filed (CRF) and spider mkey Optimization(SMO). Initially CRF is used for selecting contributed features and then SMO is applied for finalizing useful features. CNN is also used for classification of database as normal and attacks. Their system proved better in terms of detection accuracy, time and false positive rate.

Z. Wang, *et al.* [33] Proposed intrusion detection model based on deep belief network (DBN). Here in place of back propagation (BP) they used Kernel based extreme learning machine(KELM) with supervised learning for training networks also enhanced great wolf optimizer (EGWO) is used in order to optimize parameters of KELM. The datasets KDDCupgg, NSL-KDD, UNSW-NB15 and C1c!D32017 are used and shows that the algorithm they used has greater advantage in terms of accuracy, precision true positive rate, false positive rate.

M. Zeeshan, *et al.* [34] Proposed protocol based intrusion detection (PB-DID) architecture, wherein they created a dataset of packets from within the IoT traffic by doing the comparison of features from BoT-IoT and UNSWNB15 dataset. Used deep learning technique and accuracy they achieved is 96.3%.

S. Singh, *et al.* [35] Proposed multi classifier intrusion detection system (MIDS) based on deep learning algorithm that is CNN. To train and test the model UNSWNB15 dataset is used.The solution efficiency detects and alarms the backdoors analysis, DoS, Fuzzers , Generic lVorm and shellcodes and also achieves higher accuracy along with low false positives.

S. Latif, *et al.* [36] mentioned about industrial internet of things(IIoT). For intrusion detection in IIoT they made use of Deep Random Neural Network(DRaNN) and the dataset they used is UNSW-NB15. Their results proved efficient for 9 different types of attacks with accuracy of 99.54%.GD algorithm was used to train the neural network. It showed low false positive rates.

A. Dawoud, *et al.* [37] To reveal the threats they used novel anomaly detection framework that

is based on unsupervised deep learning. Proved how deep learning can be used to detect anomalies by the use of restricted Boltzmann machines against the autoencodes as non-probabilistic algorithm. Their study provided with in-depth analysis of the unsupervised deep learning. Their result shows 99% detection accuracy.

P. V. Huong, *et al.* [38] Worked on Deep learning using a Convolutional neural network. Here they worked on log information of an IoT system such as service, address, location some more which are extracted into the original feature set. Later on the original feature set is encoded and improved in form of digital matrix and gave to convolutional neural network for training and detection. It is evaluated on the basis of cross validation and has the accuracy of about 98.9%.

B. Sharma, *et al.* [39] Provided a survey of anomaly detection in IoT applications using machine learning and deep learning, they act as powerful tool in order to analyze normal and abnormal behavior in IoT. They outline the major issues and challenges by using deep learning for abnormal detection. Stated how fog computing helps to move the computation at the device or edge in order to solve the issues of network security and delay computation

Saba, T., *et al.* [40] used Convolution Neural Network (CNN) .This model utilized the advantage of IoT's power and efficiently examine the whole traffic across the IoT. Moreover, this model intelligently predicts new attacks, unlike previous threats. It did not include the DL algorithms for improving the threat detection rate.

Otoum, Y., *et al.*[41]used Spider Monkey Optimization algorithm (SMO) and the Stacked-Deep Polynomial Network (SDPN). This method was used to detect all anomalies with no significant errors. This method was not validated with different classifiers and datasets.

Jeyaselvi, M., *et al.* [42] used Look Ahead Artificial Neural Network (LAANN). In this model, the computational time was less. In real time usage, the amount of connectivity in IOT devices were increased along with the huge amount of data, which leads to tremendous security attack.

RESEARCH GAPS

After having done extensive literature review on the topic of Intrusion Detection in IoT it has been observed that there are different challenges in the existing Intrusion Detection Techniques as listed below.

- Immense benefit has brought by IoT to day to day life surrounding a various range of application fields that we frequently interrelate with, ranging from transport and smart environments to healthcare automation. Nevertheless, because of the drawback of computational capabilities and limited resources, IoT networks are prone to different cyber-attacks.
- The developed deep transfer learning approach in [1], which has the ability to classify attacks in an efficient manner however, it has the need to concentrate on many IoT sensors and optimize the hyper-parameters of the developed deep transfer learning for improved performance. In addition, the deep learning model was established on privacy-preserving decentralized servers or devices.
- The Deep Transfer Learning based IDS introduced in [3] obtained better detection rate although, the developed IDS was not deployed in real IoT environment and also there is a need to reduce the accuracy loss while optimizing it with no accuracy loss and studying its performance on real IoT network traffic data.
- Although, less time was consumed by the MCFT-CNN methodology in [4], it did not use the advantage of spatial pooling layer. Thus, it does not have the ability to utilize full-size malware image as input, so that this method failed to improve the efficiency.
- An intrusion detection approach by using auto encoders was implemented in [5], but this method did not include diverse device types in addition to computers, controllers, and roboticarms. Therefore, it needs further investigation to test the performance for more device types.

4. AIM AND OBJECTIVES

In view of above discussions, the aim of this research work is to address the issues of intrusion detection in IoT environment using deep learning methods. To fulfill the aim of the study following objectives are identified:

- To design an optimized algorithm, for cluster head selection and routing in order to solve the overfitting issues while routing.
- To develop the new Intrusion Detection Model to detect the malevolent activities that occurs in the IoT environment and to protect it from Intruders.
- To model the fitness function based on four parameters like, energy, delay, distance and trust for cluster head selection and routing to base station
- To evaluate and compare the performance of the proposed optimized algorithm with the existing algorithms.

5. RESEARCH METHODOLOGY

This section explains the intrusion detection in IoT technique using proposed hybrid optimization algorithm. This technique mainly includes following stages, initially we will be performing IoT simulation where we will get the log files gathered at nodes. Then the cluster head selection and routing will be done at base station. Features will be normalized, and mean while we will select best required features. And then finally intrusion detection will take place.

5.1 IoT simulation:

For achieving admirable intrusion detection, the IoT simulation will be performed as the initial step, where in the log file will be gathered by nodes.

5.2 Cluster head selection and routing:

Cluster head selection and routing to base station will be done by means of the proposed optimization algorithm. The new optimization algorithm is to be proposed after studying various algorithms for Cluster Head Selection.

5.3 Intrusion detection at base station:

The intrusion detection will be performed at the base station as follows. At the beginning, the data will be collected, and is fed to the next stage.

5.4 Feature Normalization:

Feature normalization will be performed by using some standard normalization technique for normalizing the feature which gives the best results.

5.5 Feature selection:

Consequently, feature selection will be performed wherein most important features will be extracted by using the distances, including Czekanowski, Minkowski or some other feature selection technique.

5.6 Intrusion detection:

Intrusion detection will be performed using CNN with transfer learning [13], where CNN will be used with the hyper parameters from trained models, like GoogLeNet [14] , ResNet-50 [15] or some other standard Model.

6. CONCLUSIONS

IoT devices has become popular over the last couple of years because of their appealing connectivity, communication, and decision- making features. The security issues of IoT attracted more attention for ensuring the security of network, the intrusion detection technology is a significant method that has turn into a demanding topic in the study of the security of IoT. For the identification of network traffic in the IoT environment, this research introduces a novel optimization algorithm. At first, the IoT will be simulating, then the nodes will collect log file. After that, the cluster head selection and routing to base station will be done. Finally, the CNN will be used with the hyper parameters from trained models. This model will be using the characteristics of the new optimization algorithm in order to achieve better performance. The metrics energy, precision, recall and F-measure of this work will be measured and the performance of the proposed method will be compared to the existing methods.

REFERENCES

[1] Mehedi, S.T., Anwar, A., Rahman, Z., Ahmed, K. and Rafiqul, I., "Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach", IEEE Transactions on Industrial Informatics, April 2022.

[2] Raj, J.S. and Basar, A., "QoS optimization of energy efficient routing in IoT wireless sensor networks", Journal of ISMAC, Vol.1, No.01, pp.12-23, June 2019.

[3] Paxson, V., "Bro: a system for detecting network intruders in real-time", Computer networks, Vol.31, No.23-24, pp.2435-2463, December 1999.

[4] Roesch, M., "Snort: Lightweight intrusion detection for networks", In Lisa, Vol. 99, No. 1, pp. 229-238, November 1999.

[5] Atefinia, R. and Ahmadi, M., "Network intrusion detection using multi-architectural modular deep neural network", The Journal of Supercomputing, Vol.77, No.4, pp.3571-3593, April 2021.

[6] Weiss, K., Khoshgoftaar, T.M. and Wang, D., "A survey of transfer learning", Journal of Big data, Vol.3, No.1, pp.1-40, December 2016.

[7] Agarwal, N., Sondhi, A., Chopra, K. and Singh, G., "Transfer learning: Survey and classification", Smart innovations in communication and computational sciences, pp.145-155, 2021.

[8] Chen, C.M., Chen, Y.L. and Lin, H.C., "An efficient network intrusion detection", Computer communications, Vol.33, No.4, pp.477-484, March 2010

[9] De la Hoz, E., De La Hoz, E., Ortiz, A., Ortega, J. and Prieto, B., "PCA filtering and probabilistic SOM for network intrusion detection", Neurocomputing, Vol.164, pp.71-81, September 2015.

[10] Al-Yaseen, W.L., Othman, Z.A. and Nazri, M.Z.A., "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system", Expert Systems with Applications, Vol.67, pp.296-303, January 2017.

[11] Kevric, J., Jukic, S. and Subasi, A., "An effective combining classifier approach using tree algorithms for network intrusion detection", Neural Computing and Applications, Vol.28, No.1, pp.1051-1058, December 2017.

[12] Sahu, S. and Mehtre, B.M., "Network intrusion detection system using J48 Decision Tree", In Proceedings of 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2023-2026, IEEE, August 2.

[13] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M.A. and Lu, S., "IoT intrusion detection system using deep learning and enhanced transient search optimization", IEEE

Access, Vol.9, pp.123448-123464, August 2021.
[14] Idrissi, I., Azizi, M. and Moussaoui, O., “Accelerating the update of a DL-based IDS for IoT using deep transfer learning”,Indones. J. Electr. Eng. Comput. Sci., Vol.23, No.2, pp.1059-1067, August 2021.
[15] Tien, C.W., Huang, T.Y., Chen, P.C. and Wang, J.H., “Using Autoencoders for Anomaly Detection and Transfer Learning in IoT”, Computers, Vol.10, No.7, p.88, July 2021.
[16] Deng, L., Li, D., Yao, X. and Wang, H., “Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm”, Cluster Computing, Vol.22, No.4, pp.9889-9904, July 2019.
[17] Sudhakar & Kumar, S., “MCFT-CNN: Malware classification with fine-tune convolution neural networks using traditional and transfer learning in Internet of Things”, Future Generation Computer Systems, Vol.125, pp.334-351, 2021.
[18] Ge, M., Syed, N.F., Fu, X., Baig, Z. and Robles-Kelly, A., “Towards a deep learning-driven intrusion detection approach for Internet of Things”, Computer Networks, Vol.186, p.107784, February 2021
[19] Ullah, I. and Mahmoud, Q.H., “Design and development of a deep learning-based model for anomaly detection in IoT networks”, IEEE Access, Vol.9, pp.103906-103926, July 2021.
[20] Nayak, S., Ahmed, N. and Misra, S., “Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things”, Ad Hoc Networks, Vol.123, p.102661, December 2021.
[21] Ayyarao, T.S., RamaKrishna, N.S.S., Elavarasan, R.M., Polumahanthi, N., Rambabu, M., Saini, G., Khan, B. and Alatas, B., “War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization”,IEEE Access, Vol.10, pp.25073-25105, February 2022.
[22] Kaveh, A. and Zaerreza, A., “Shuffled shepherd optimization method: a new meta-heuristic algorithm”, Engineering Computations, March 2020
[23] Jain, Y.K. and Bhandare, S.K., “Min Max Normalization Based Data Perturbation Method for Privacy”, Int. J. Comput. Commun, Vol.4, pp.233-238, 2013.
[24] Shi, Z., Hao, H., Zhao, M., Feng, Y., He, L., Wang, Y. and Suzuki, K., “A deep CNN based transfer learning method for false positive reduction”, Multimedia Tools and Applications, Vol.78, No.1, pp.1017-1033, January 2019.
[25]] He, K., Zhang, X., Ren, S. and Sun, J., “Deep residual learning for image recognition”, In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770-778, 2016.

[26] BoT-IoT dataset will be taken from “https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php”, accessed on August 2022.
[27] Y. Zhang*, Peisong Li and Xinheng Wang, “Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network”, In Journal IEEE, February 2019.
[28] A. Nagisetty, Govind P. Gupta, “Framework for Detection of Malicious Activities in IoT Networks using Keras Deep Learning Library”, Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019, ISBN: 978-1-5386-7808-4, IEEE.
[29] M. Zeeshan, Q. Riaz, M. A. Bilal, Muhammad K. Shahzad, H. Jabeen, S. A.Haider, A. Rahim, “Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Set”, VOLUME 10, IEEE December 2021.
[30] S.Shinly Swarna Sugi, Dr.S.Raja Ratna, “Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network”, Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020] .
[31] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, , “Network Intrusion Detection for IoT Security based on Learning Techniques”, IEEE Communications Surveys And Tutorials, Vol. 00, No. 0, November 2018.
[32] Mrs.G.Parimala , Dr.R.Kayalvizhi, “An Effective Intrusion Detection System for Securing IoT Using Feature Selection and Deep Learning”, 2021 International Conference on Computer Communication and Informatics (ICCCI -2021).
[33] Z. Wang , Y. Zeng, Y. Liu , And D. Li, “Deep Belief Network Integrating Improved Kernel-Based Extreme Learning Machine for Network Intrusion Detection”, VOLUME 9, 2021.
[34] M. Zeeshan, Q. Riaz , M. A. Bilal , M. K. Shahzad , H. Jabeen2, Syed Ali Haider , And A. Rahim, “Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets”, VOLUME 10, 2022.
[35] S. Singh, S. V. Fernandes, “MCIDS-Multi Classifier Intrusion Detection system for IoT Cyber Attack using Deep Learning algorithm”, Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).

[36] S. Latif, S. Latif, Z. Zou, J. Ahmad, “DRaNN: A Deep Random Neural Network Model for Intrusion Detection in Industrial IoT”, October 05,2020.

[37] A. Dawoud, O. A. Sianaki, S. Shahristani, C. Raun, “Internet of Things Intrusion Detection: A Deep Learning Approach”, 2020 IEEE Symposium Series on Computational Intelligence (SSCI) December 1-4,2020.

[38] P. V. Huong, Le D. Thuan, Le Thi H. Van, D. V. Hung, “Intrusion Detection in IoT Systems Based on Deep Learning Using Convolutional Neural Network”, 2019 6th NAFOSTED Conference on Information and Computer Science (NICS).

[39] B. Sharma, L. Sharma, C. Lal, “Anomaly Detection Techniques using Deep Learning in IoT: A Survey”, 2019 International Conference on Computational Intelligence and Knowledge Economy(ICCIKE).

[40] [40] Saba, T., Rehman, A., Sadad, T., Kolivand, H. and Bahaj, S.A., “Anomaly-based intrusion detection system for IoT networks through deep learning model”, Computers and Electrical Engineering, vol.99, pp.107810, 2022.

[41] Otoum, Y., Liu, D. and Nayak, A., “DL-IDS: a deep learning–based intrusion detection framework for securing IoT”, Transactions on Emerging Telecommunications Technologies, 33(3), pp. e3803, 2022.

[42] Jeyaselvi, M., Dhanaraj, R.K., Sathya, M., Memon, F.H., Krishnasamy, L., Dev, K., Ziyue, W. and Qureshi, N.M.F., “A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks”, Cluster Computing, vol.26, no.1,pp.559-574,2023.